

Internet : quelques conseils et précautions

Résumé : comme tout outil, internet peut se révéler formidable ou terrible. Les quelques conseils ci-dessous vous permettront d'en tirer le meilleur parti, et surtout d'éviter les pièges et les erreurs grossières, notamment les virus et le spam tout en protégeant votre vie privée.

Introduction

L'informatique et internet sont des outils, donc ils peuvent vous apporter des choses formidables d'un côté, et se révéler dangereux de l'autre. Et comme tous les outils, il est possible d'apprendre à s'en servir. Cet article est fait pour ça, pour les aspects liés à votre vie privée, votre présence sur internet via votre adresse email et vos participations à des sites web.

J'utilise internet depuis 1995, quand j'étais étudiant. Depuis cette année là, j'ai toujours eu la chance d'être connecté en haut débit et avec une connexion illimitée en temps (autrement dit je n'ai pas eu besoin d'utiliser un modem bas débit facturé au temps de connexion) : réseau de l'éducation nationale, câble, puis ADSL. De plus, je travaille dans les télécoms et l'informatique, internet est mon métier.

C'est grâce à cette expérience que je peux vous donner les quelques conseils ci-dessous. Ils sont valables pour tous les sites web et internet en général, seul le dernier paragraphe est spécifique au Cactus Francophone.

Internet

Bien souvent, quand on dit *internet*, on pense en fait au *web* : les nombreux sites sur lesquels nous passons du temps, avec un logiciel appelé *navigateur*, comme internet explorer, Mozilla Firefox ou autre (il y en a plein).

Mais ce n'est pas tout ! Internet, c'est aussi l'email (le courrier électronique), les échanges de fichiers (par FTP ou P2P), les newsgroups, etc. Cet article va principalement parler du web et de l'email, les 2 utilisations les plus courantes pour le grand public.

Le web

Un site web est d'abord un moyen de diffuser une information, par exemple : un CV ou des photos pour un particulier, une plaquette de présentation pour une entreprise, etc. Puis c'est devenu un moyen d'intéragir avec le visiteur, par le moyen des forums de discussion, des catalogues de vente, des wikis, des réseaux sociaux (Facebook, MySpace, LinkedIn, ...) etc.

Les usages du web n'en sont qu'à leurs débuts, les possibilités sont énormes.

Comme il y a échange d'informations entre votre ordinateur et le serveur qui fait fonctionner les sites web visités, il peut parfois y avoir un risque pour votre système, j'y reviens ci-dessous.



Pour en savoir plus : [Web sur Wikipedia](#)



L'email

Le courrier électronique a été pensé comme le classique courrier papier, avec en plus les avantages qu'apporte l'informatique : le transfert quasi instantané, la possibilité d'envoyer un même courrier à plusieurs personnes d'un coup, la copie et le transfert d'un simple clic, etc.

Ce qui était parfois fastidieux avec le courrier *papier* devient trivial avec l'informatique, avec les avantages et inconvénients que ça implique :

- vous pouvez envoyer la photo du petit dernier à toute votre famille d'un simple clic, même si votre famille compte 115 frères, soeurs, oncles, tantes, cousins, etc.
- n'importe qui peut vous écrire sans que ça lui coûte cher, d'où de la publicité fréquente.



Pour en savoir plus : [Courrier électronique sur Wikipedia](#)



Les dérives

Les principales dérives dont je vais vous parler sont les **virus** et le **spam**, et je vais vous expliquer comment vous en prémunir.

Internet permet donc de faire bien des choses, parfois géniales, parfois déplorables. Bien des maux lui sont reprochés, mais gardez à l'esprit que c'est juste un outil qui permet de faciliter ce qui se faisait déjà avant.

Le SPAM

Les **courriers indésirables** sont aussi appelés SPAM ou pourriels. Les plus courants vous proposent des pilules pour maigrir, pour avoir un plus gros sexe, pour vous enrichir rapidement, pour obtenir des crédits fabuleux, etc. Il s'agit de messages non sollicités qui polluent votre boîte aux lettres, et les

autocollants **StopPub** sont sans effet ici



Grâce à l'informatique et à internet, il est techniquement possible d'envoyer des millions de courriers pour un coût très faible, et en plus de le faire sans l'accord des destinataires. Les spammeurs ont des bases de données contenant des millions et des millions d'adresses email, qu'ils utilisent sans vergogne pour nous inonder de leurs publicités ou tentatives d'arnaques.

Pour se protéger de ce fléau qu'est le spam, il faut travailler sur 2 axes :

1. protéger son adresse email pour qu'elle ne figure pas dans les bases de données des spammeurs
2. avoir un bon logiciel de filtrage, capable de détecter automatiquement les messages indésirables et de les supprimer.

Sachez qu'à partir du moment où une adresse email est utilisée, le spam est inévitable, ce n'est qu'une question de temps (voir les explications ci-dessous). Prendre des précautions peut ralentir et limiter, mais pas éviter.



Pour en savoir plus : [Pourriel sur Wikipedia](#)

Précautions

Les spammeurs ont des programmes, aussi appelés robots de collecte, qui parcourent les pages web automatiquement pour repérer les adresses email. Ils les entrent alors dans leurs bases de données. Mais il est nécessaire, pour utiliser certains sites web, de fournir votre adresse email, et souvent elle peut alors être visible, soit par tous les visiteurs du site qui iront sur votre fiche de membre par exemple, ou seulement les membres du site. Comment éviter alors qu'elle soit récoltée puis utilisée pour le spam ?

Votre adresse email est une donnée personnelle qu'il faut protéger des spammeurs. Contrairement à votre adresse postale, vous pouvez avoir plusieurs adresses emails : l'idée est alors de créer une adresse email qui ne vous servira qu'à tous ces sites qui vous la demande, et qui font plus ou moins d'efforts pour la protéger. Vous pouvez utiliser pour ça les webmails gratuits, comme [GMail](#).

Conseil n°1

Utiliser 2 adresses email :

- * une pour vos proches, que vous communiquez peu
- * une pour votre activité sur le web, faite exprès pour ça

Avec Gmail (et sans doute d'autres webmail), vous pouvez demander à votre logiciel de lecture habituel de courrier (Mozilla Thunderbird, ms-outlook, etc) d'aller y chercher les messages, comme ça vous n'avez pas besoin d'utiliser plusieurs logiciels.

Comme expliqué ci-dessous dans le chapitre sur les virus, vous finirez forcément par recevoir du spam, quelque soient les précautions prises. Il existe de bons outils anti-spam, aussi bien sur les webmails que pour les logiciels de lecture de courrier.

J'utilise pour ma part 2 filtre anti-spam successifs : d'abord GMail, qui est très très efficace, puis Mozilla Thunderbird, un logiciel libre et gratuit de lecture de courriers qui a un filtre anti-spam intégré.

Conseil n°2

Utiliser un anti-spam efficace, par exemple celui de GMail ou celui de Mozilla Thunderbird.

Les solutions payantes ne sont pas réputées ni prouvées plus efficaces.

C'est trop tard !

Si vous ne saviez pas tout ça, et que vous n'avez qu'une seule adresse email qui est maintenant pourrie par le spam et utilisée un peu partout sur internet, que faire ? Le plus simple est de la laisser tomber, et de créer 2 nouvelles adresses : 1 personnelle (par exemple prenom.nom@gmail.com) et une pour vos activités sur le web (par exemple pseudo1515@gmail.com).

Et si vous préférez avoir tous vos messages dans un seul logiciel, prenez par exemple Mozilla Thunderbird et demandez-lui d'aller chercher vos messages sur toutes vos différentes adresses.

Les virus

Les virus informatiques jouent un rôle primordial dans le spam :

Au départ, les virus informatiques étaient des programmes créés pour s'amuser, le but étant de faire des concours d'infection : le programmeur qui infectait le plus de machines avait gagné. Les virus sont maintenant utilisés à des fins crapuleuses : d'abord prendre le contrôle d'une machine (votre ordinateur) pour ensuite lui faire faire plusieurs choses :

1. récolter toutes les adresses email qui se trouvent sur le disque dur : la votre, mais aussi celle de toutes les personnes qui sont dans votre carnet d'adresse, et dans tous les messages reçus et envoyés. Ces adresses servent ensuite au spam bien sûr.
2. envoyer du spam : les ordinateurs infectés servent à envoyer des messages par millions, car même si ça ne coûte pas grand chose, ça coûte pas mal quand il faut en envoyer des dizaines de millions.
3. attaquer d'autres ordinateurs, soit pour les infecter et poursuivre le cycle, soit pour faire du chantage au déni de service.

Quand un virus est installé sur votre ordinateur, il va essayer de se propager. L'un des moyens consiste à s'envoyer lui-même à tous vos contacts, dans un message avec une pièce jointe : par exemple un petit programme appelé `feu-d-artifice.exe`, qui va en effet afficher une jolie animation, tout en infectant le windows des personnes qui l'auront exécuté. Il peut aussi s'agir de fichiers plus banals, comme des photos ou des textes, présentations, pdf, qui vont profiter de failles dans les logiciels comme microsoft office, adobe pdf reader, etc. Il ne faut pas ouvrir les pièces jointes inattendues ! En cas de doute, demandez à votre contact s'il a bien envoyé le fichier et vérifiez-le avec votre antivirus à jour.

On voit ici que même si vous n'utilisez pas votre adresse email sur des sites internet, il suffit que l'ordinateur d'une personne à qui vous avez écrit ou qui vous a écrit soit infecté pour que votre email soit dans les bases de spammeurs. C'est inévitable quelque soient les protections que vous prendrez.

Tôt ou tard, votre adresse email sera dans les bases de données des spammeurs.

Conseil n°3

Si vous utilisez microsoft windows, gardez un antivirus à jour, et n'ouvrez pas les fichiers douteux reçus par email.

Je ne pourrai pas vous conseiller plus dans ce domaine car j'utilise Linux, un système d'exploitation plus performant que ms-windows, et pour lequel il n'est pas nécessaire d'utiliser un anti-virus. Vous aussi pouvez utiliser Linux, mais ce n'est pas le propos de cet article.

Votre vie privée

Vous savez maintenant comment protéger un peu mieux votre adresse email du spam, mais ce n'est pas tout. À partir du moment où vous avez une *activité en ligne*, même une simple participation à une discussion sur un petit forum, il faut protéger votre vie privée.

Il suffit simplement d'avoir un peu de bon sens, et de ne pas faire sur internet ce que vous ne feriez pas dans la rue. Ça peut sembler être une lapalissade, mais parfois le confort d'un fauteuil bien

installé derrière un écran d'ordinateur peut conduire à se laisser aller à quelques imprudences. On se retrouve alors à publier en ligne des informations qu'on ne dirait pas dans la rue à de parfaits inconnus !

Faisons d'abord une petite expérience : commencez par chercher ce qui existe à votre sujet sur internet, en vous cherchant sur google et autres moteurs de recherche. Mettez votre nom et votre prénom, en essayant plusieurs combinaisons. Exemple :

```
Prénom Nom  
"Prénom Nom"  
"Nom Prénom"
```

Demandez-vous si vous seriez gêné que quelqu'un d'autre trouve ces informations : vos amis, votre famille, vos collègues de travail, vos voisins, un employeur potentiel, etc. Puis gardez à l'esprit ce que vous ne voudriez pas que quelqu'un trouve sur vous quand vous participez à un forum, un réseau social, quand vous publiez des photos, etc.

Pourquoi se protéger

Certaines informations sont anodines : demander des conseils de culture sur une plante à piquants ne vous expose pas à grand chose. Publier des photos de sorties festives où vous finissez la soirée dans le caniveau peut donner une mauvaise image de vous. Là, c'est à chacun de voir en fonction de lui, il n'y a pas de règle générale. Voici un autre exemple :

- vous écrivez sur un forum médical pour un problème de santé, tout en cherchant un travail : un employeur qui recevrait votre CV pourrait alors se dire qu'il vaut mieux ne pas vous embaucher. Et ça, même si vous posez la questions par curiosité, pour un ami ou un membre de votre famille, etc.

Sachez que quasiment tout ce qui est publié sur internet est indexé, enregistré par les moteurs de recherche, et peut ensuite être retrouvé par n'importe qui.

Précautions

Sachant ça, à vous de décider de ce que vous posterez sur internet, et comment. Pour participer à un forum où vous parlerez de choses privées et personnelles, par exemple un forum sur la santé, utilisez une adresse email qui ne contient pas vos noms et prénoms, et utilisez un pseudo (ou juste votre prénom s'il est courant).

Sur le Cactus Francophone

Et le Cactus Francophone dans tout ça ? Comment y est gérée la vie privée des membres ?

Tout d'abord, il est possible de participer au forum sans être inscrit, sans donner d'adresse email : un pseudo suffit. C'est très rare maintenant sur internet, il faut en général au moins s'inscrire. Devenir membre permet d'avoir un suivi de ses messages, de réserver son pseudo, et autres avantages : il suffit de choisir un pseudo et de donner une adresse email valide. C'est tout. Il est ensuite possible,

sur sa fiche de membre, de décider ou non de publier cette adresse email, qui sera de toutes façons protégée contre la récolte (même si aucune protection n'est infaillible).

Vous pouvez ensuite décider de donner plus d'informations sur vous, ou pas : nom, prénom, descriptif, site web, etc. Mon conseil est de donner au moins :

- le prénom, c'est plus sympa
- le pays et la région, pour les conseils de culture
- un descriptif des plantes que vous cultivez et que vous préférez

Mais c'est vous qui voyez :)

Liens pour aller plus loin

- [Choisir un bon mot de passe](#)

Conclusion

Faites attention à vos données personnelles, protégez votre vie privées. De simples précautions suffisent pour qu'internet soit un outil pratique sans devenir dangereux ni gênant.

Date de publication : 2009-06-06

Auteur : [Yann Cochard](#)

Licence : **CC BY-SA** (résumé : vous avez le droit de reproduire, distribuer et communiquer ce texte, de le modifier, aux conditions suivantes : conserver le nom de l'auteur, et donner les mêmes droits aux personnes à qui vous le distribuez)

From:

<https://www.cactuspro.com/articles/> - **Articles du Cactus Francophone**

Permanent link:

<https://www.cactuspro.com/articles/hors-sujet/internet-quelques-conseils-et-precautions>

Last update: **2009/06/10 06:17**

